Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of adding elements of a finite field F_{2^m}, where m is less than a predetermined number n, said method comprising the steps of:

a) storing a first and a second element in a pair of registers, each of said pair of registers comprising said predetermined number of machine words;

b) establishing an accumulator having said predetermined number of machine words; and

c) computing for each of said machine words in said accumulator the exclusive-or of the corresponding machine words representing each of said first and second elements to obtain a representation of a result of the addition of said elements, and, upon completion of said computation, performing a modular reduction to reduce said result to a predetermined number of words.

2. (cancel)

3. (original) A finite field multiplier operable to multiply two elements of one of a plurality of finite fields, said finite fields being partitioned into subsets, said multiplier comprising:

a) a plurality of wordsized finite field multipliers, each suitable for multiplying elements of each finite field in a respective subset of said plurality of finite fields;

b) a finite field reducer configured to perform reduction in said one finite field;

c) a processor configured to

i) operate the wordsized finite field multiplier suitable for use with said one finite field to obtain an intermediate product; and

ii) operate said finite field reducer on said intermediate product to obtain the product of the two elements.

4. (currently amended) A method of performing a finite field operation on [[two]] at least one element[[s]] r, [[s]] of a finite field, comprising the steps of:

a) representing each element as a number of machine words;

b) [[a)]] performing a wordsized operation on said representations of [[r and s]], said wordsized operation corresponding to said finite field operation;

c) completing said wordsized operation for each word of said representations to obtain a

result; and

d) [[b)]] performing a modular reduction of [[the]] said result to reduce said result to a predetermined number of words. ~~of step a);~~

5. (original) A finite filed engine for performing a finite field operation on at least one element of a finite field chosen from a set of finite fields, said set of finite fields being divided into subsets according to their word size, comprising:

a) a finite field operator for each of said subsets;

b) a finite field reducer for each of said finite fields;

c) a processor configured to choose the finite field operator corresponding to the subset containing said chosen finite field and the finite field reducer for said chosen finite field and apply the chosen finite field operator to said element to produce an intermediate result and apply the chosen finite field reducer to said intermediate result to obtain the result of said finite field operation.

6. (currently amended) A cryptographic system comprising:

a) a plurality of elliptic curves, each specifying elliptic curve parameters and a respective finite field;

b) a plurality of finite field settings corresponding to each finite field;

c) a plurality of wordsized finite fields, each having routines, each finite field being assigned to one of said wordsized finite fields;

d) a reduction routine for each finite field;

e) a computational apparatus configured to perform a cryptographic operation by the steps of:

i) selecting one of said elliptic curves; and

ii) performing a cryptographic function using the routines from the wordsized finite field to which the respective finite field corresponding to said selected elliptic curve is assigned; said routines including at least one finite field operation and, subsequent thereto, a modular reduction to obtain a result of said operation corresponding to a predetermined number of words.

7. (new) A method according to claim 4 wherein said modular reduction is determined by said finite field.

8. (new) A method according to claim 4 wherein said finite field operation is addition.

9. (new) A method according to claim 4 wherein said finite field operation is subtraction.

10. (new) A method according to claim 4 wherein said finite field operation is multiplication.

11. (new) A method according to claim 4 wherein said finite field operation is division.